United States Attorney
Southern District of New York

FOR IMMEDIATE RELEASE
July 12, 2004

CONTACT: **U.S. ATTORNEY'S OFFICE**
MARVIN SMILON, HERBERT HADAD
MEGAN GAFFNEY
PUBLIC INFORMATION OFFICE
(212) 637-2600

U.S. INDICTS WESTCHESTER MAN FOR ACCESSING VERIZON COMPUTERS WITHOUT AUTHORIZATION

DAVID N. KELLEY, the United States Attorney for the Southern District of New York, announced the indictment today of WILLIAM QUINN, 27, of East Chester, New York, on charges of gaining unauthorized access to computers of Verizon Communications, Inc. The indictment alleges that, from at least in or about January 2004 through and including April 2004, QUINN obtained unauthorized access to Verizon's Direct Access Testing Units (DATUs)——computers that disable Verizon telephone numbers while performing a series of tests on a telephone line——and instructing others on Internet websites on how to do the same. To restore the security of its nationwide telephone network, Verizon was forced to spend hundreds of thousands of dollars.

Verizon Communications, Inc. ("Verizon") provides local telephone service in the Southern District of New York and elsewhere. In addition to servicing numerous residential and business customers, Verizon provides telephone service for 911 emergency operators, fire departments, police departments,

hospitals, and other critical infrastructure in the Southern District of New York and elsewhere.

The Indictment alleges that, to enable its employees to test and repair its telephone lines remotely, Verizon utilizes Direct Access Testing Units ("DATUs") in each telephone area code in which it operates. A DATU is a computer connected to a group of "test" telephone lines that mirror (or run parallel to) all active telephone lines in a particular area code. Each DATU is accessed through a unique telephone number. If a Verizon employee wishes to test or repair a particular telephone number/line remotely, the Verizon employee dials the telephone number for the appropriate DATU, inputs a multi-digit password to gain access to the DATU computer system, and then sends numeric and other commands telephonically to the DATU that (1) disconnect the tested telephone number/line from outside access (the active number/line), and (2) re-connect that number/line to the "test line." From there, the Verizon employee can perform any number of tests to the line or repair problems on the line by sending additional numeric and other commands telephonically to the DATU. While the active number/line is being tested via the DATU, it is disabled from receiving or making any calls. Accessing a telephone line via a DATU, in short, renders a telephone number/line inoperable during the testing process.

The Indictment alleges that, beginning at least in or about January 2004, WILLIAM QUINN and others posted the passwords

to various Verizon DATUs — along with instructions on how to use the passwords to obtain unauthorized access to Verizon's DATUs — on Internet websites devoted to "phreaking" (the practice of obtaining unauthorized use of telecommunications services). According to the Indictment, QUINN and his fellow "phreakers" encouraged others — in audio and text messages posted on the Internet — to access Verizon's DATUs without authorization. The Indictment alleges that QUINN used those passwords to obtain unauthorized access to Verizon DATUs. Between in or about late January 2004 and in or about April 2004, QUINN accessed and attempted to access Verizon DATUs from his home in the Southern District of New York at least 100 times. In so doing, QUINN allegedly acquired the same ability as an authorized Verizon employee to test and disable telephone numbers within various telephone area codes across the country.

The Indictment further alleges that, in response to the unauthorized intrusions of QUINN and others, Verizon was forced to spend at least $120,000 to restore the security of its DATU systems. For instance, among other things, Verizon was forced (a) to change the telephone numbers for each of its DATUs across the country; and (b) to pay employees overtime to reprogram the multi-digit passwords for each of those DATUs.

If convicted on the charge in the Indictment, QUINN faces a maximum prison sentence of 5 years and a maximum fine of $250,000 or twice the gross loss to the victim.

QUINN is presently released on bail after being arrested pursuant to a criminal complaint on April 29, 2004. Following today's indictment, QUINN's case was assigned to United States District Judge LORETTA A. PRESKA, who scheduled an arraignment for QUINN on July 15th at 3:30 p.m.

Mr. KELLEY praised the efforts of the United States Secret Service Electronic Crimes Task Force in conducting the investigation.

Assistant United States Attorney STEPHEN MILLER is in charge of the prosecution.

The charges contained in the Indictment are merely allegations, and the defendant is presumed innocent unless and until proven guilty.

04-143__ ###